Module Fourteen

Documentation

This module describes the various documents that a vendor may be required to supply in support of the evaluation of a trusted product. The purposeand contents of each document are described.

Module Learning Objectives

This module describes the documentation that is used to support thetrusted product development cycle described in Module 4. It presents some information that builds on material presented in Module 13. Upon completion of this module, the student should:

1. Understand the purpose and contents of each document that may be required in support of the development of a trusted system.

Overview

Documentation records the what, the how, and the why of a system implementation. It facilitates discussion and increases the level of understanding between developers themselves, and instructs and provides reference material to evaluators and end users. A trusted system will not operate in a secure manner if it is installed or used incorrectly byusers who are not provided with necessary documentation. The TCSEC specifies requirements for four types of documentation: a Security Features User's Guide (SFUG), a Trusted Facility Manual (TFM), test documentation, and design documentation.

Security Features User's Guide

An SFUG describes the protection mechanisms provided by the TCB and how they interact with one another. The document provides guidelines on the use of protection mechanisms from the standpoint of the general user of the trusted system. It should include an overview of MAC, DAC, Audit, I&A, and all other security mechanisms that impact the user. The SFUG should give tutorial information on the use of these mechanisms and the manner in which they may interact. The TCSEC requires an SFUG for all classes.

Trusted Facility Manual

The TFM provides detailed discussions of the mechanisms and protection features enforced by the TCB, and provides guidelines on their use from the standpoint of the administrative and privileged users of the trustedsystem. It should include descriptions of privileged user functions, particular TCB structures (e.g., password file), TCB generation mechanisms, and start-up procedures. The TFM and SFUG together describe the external interface to the TCB.

At class C1, the TCSEC requires a TFM that presents cautions aboutfunctions and privileges that affect security. Class C2 requires the addition of descriptions of the procedures for examining and maintaining the auditfiles . Class B1 additionally requires that the TFM describe the operator and administrator functions related to security. Guidelines on the protection features of the system, generation of a new TCB, and the control of security-related facility procedures and privileges must also be included. Class B2 requires that the TFM also identify the TCB modules that contain the reference validation mechanism (RVM) and the procedures for generation of a new TCB. Class B3 requires that the TFM add the procedures for ensuring trusted recovery.

Test Documentation

Test documentation includes all documentation that was generated in performing the testing of the TCB. This documentation should include a complete test plan describing the strategy, coverage, and environmental requirements of the test procedures, and a test results report. Test documentation must clearly indicate what aspects of the system are and are not tested by the test cases in the test suite. Those features that are not tested by the test suite are clearly candidates for additional analysis.

Class C1 requires that the system developer provide test documentationthat describes the test plan, test procedures, and results of the testing of security mechanism functionality. Classes C2 and B1 require specific additional test documentation as described in [VTD94]. Class B2 requires the additional results of covert channel bandwidth reduction testing. Class A1 requires that the test documentation also include the results of the mapping between the Formal Top-Level Specification (FTLS) and TCB source code.

Design Documentation

Design documentation communicates the design of a system and provides a rationale as to why a system is designed the way that it is. It provides an explanation of how the security policy of a system is translated intoTCB hardware, software, and firmware. It also describes the internal workings of the TCB and includes an explanation of the developer's philosophy of protection. At higher TCSEC classes, design documentation includes a model of the system's security policy and a top-level specification thatdefines the TCB interface. This documentation, then, presents the system objectives (in terms of assertions about what the system will or will not do) and thesystem functions (visible through the TCB interfaces) that ought to besubjected to security testing. This documentation encourages assessment of the completeness and correctness of the implementation. It permits anevaluation of the effect a change may have on the security of the system prior to the change being performed.

Class C1 requires that design documentation describe the manufacturer's philosophy of protection and how the TCB meets this philosophy. Classes C2 and B1 require specific additional design documentation as described in [VDD94]. Class B1 requires the addition of an informal or formaldescription of the security policy model and arguments as to why this model meets the security policy. Identification of the specific TCB protection mechanisms that satisfy the model also must be included. Class B2 requires that the design documentation include a formal description of the security policy model that must be proven to sufficiently enforce the security policy. A Descriptive Top-Level Specification (DTLS) must be provided and shown to be anaccurate description of the TCB interface. The TCB structure must be shown to facilitate testing and the enforcement of least privilege, and the results of a covert channel analysis must be presented. Class B3 requires that the TCB implementation be informally shown to be consistent with the DTLS. Class A1 requires that the TCB implementation be informally shown to beconsistent with a FTLS, and that mechanisms internal to the TCB be clearly described.

Relevant Trusted Product Evaluation Questionnaire Questions

2.14 OTHER DOCUMENTATION

C1:

1. (a) Describe the methodology used in the design of the system.(b) Provide a list of documents that capture the system design. (c)For each document, provide a copy, a brief description of its contents, or an annotated outline. (d) Provide a schedule for developmentof the design documents.
2. Does the SFUG describe (a) the protection mechanisms provided by the TCB, (b) guidelines on their use, and (c) how theyinteract?
3. Does the SFUG explain to users the underlying philosophy of protection for the system?
4. Does the SFUG discuss the need for exercising sound security practices in protecting the information processed and/or stored in the system, including all input and output?
5. Does the SFUG describe users' responsibilities with respect to assuring the effectiveness of the protective features (e.g., password selection and protection)?
6. Does the SFUG describe security-related commands available to users?
7. Does the SFUG explain how to use the DAC mechanism(s) provided by the system to protect objects?
8. Does the SFUG explain how removable media are to be handled (if applicable)?
9. Does the SFUG discuss the auditing of security-relevant events?
10. Does the SFUG include and clearly highlight warnings where needed?
11. (a) Does the TFM contain procedures to configure the secure system? (b) Does it list the devices and hardware elements that are part of the evaluated configuration? Does it contain procedures (c) for configuring each of the devices, (d) for connecting them, and (e) for configuring the entire system?(f) Does it list the devices that are not part of the evaluated configuration? (g) Does it list the procedures for securely configuring them out and for disconnecting them?
12. Does the TFM list the (a) functions, (b) privileges, and(c) data bases that are to be controlled? (d) Does it describe how theseare

controlled? (e) Does it describe the consequences of granting access to them as warnings?

13. (a) Does the TFM contain the procedures and warnings relating to the secure operation of the computing facility? (b) Does it address the physical, personnel, and administrative aspects of security in order to ensure the protection of computing hardware, firmware, software, and privileged devices such as the operator terminals?

14. Does the TFM contain the procedures for securely starting/ booting/ initializing the system?

C2:

15. (a) Does the TFM provide procedures for maintaining the audit log? (b) Does it describe how the audit log can be turned on,turned off, combined with other audit logs, and backed up? (c) Does it describe how to detect that the audit log is getting full, or is full, and what actions to take in order to minimize the loss of audit data?

16. Does the TFM contain the (a) structure of the audit log file and the (b) format of the audit records? (c) Does it describe howthe audit records can be viewed? Does it (d) describe the capabilities of the audit reduction tool, (e) how to invoke these capabilities, and (f) the format of the tool output?

B1:

17. Does the TFM address the protection of hard-copy outputs?

18. (a) Does the TFM provide a list of trusted users (e.g., system operator, security administrator, accounts administrator, auditor) and trusted processes (device queue manipulation, user profile editor)? (b) For each trusted user or process, does itlist the functions (e.g., creating and deleting users, changing user security profile, setting up defaults for discretionary and mandatory access controls, selecting auditing events), privileges, and data bases (e.g., user security profiles, authentication data base) to be accessed?

B2:

19. (a) Does the TFM contain procedures to generate the TCB from source code? (b) For each system parameter or input, does the TFM list valid values for a secure TCB generation?

20. Does the TFM include a list of TCB modules that make up the security kernel?

21. Are the separate operator and administrator functions clearly identified and described?

B3:

22. Does the TFM contain the procedures for securely restarting/ resuming the system after a lapse in system operation, or a system failure?

Required Readings

TCSEC85 National Computer Security Center, *Department of Defense Trusted Computer Security Evaluation Criteria*, DoD 5200.28-STD, December 1985.

There are numerous TCSEC requirements related to documentation. Each documentation type is listed below along with the Sections where its requirements appear in the TCSEC:

- SFUG: 2.1.4.1, 2.2.4.1, 3.1.4.1, 3.2.4.1, 3.3.4.1, and 4.1.4.1 (summarized on page 104).
- TFM: 2.1.4.2, 2.2.4.2, 3.1.4.2, 3.2.4.2, 3.3.4.2, and 4.1.4.2 (summarized on page 107).
- Test Documentation: 2.1.4.3, 2.2.4.3, 3.1.4.3, 3.2.4.3, 3.3.4.3, and 4.1.4.3 (summarized on page 106).
- Design Documentation: 2.1.4.4, 2.2.4.4, 3.1.4.4, 3.2.4.4, 3.3.4.4, and 4.1.4.4 (summarized on pages 97-98).

INTERP94 National Computer Security Center, *The Interpreted TCSEC Requirements*, (quarterly).

The following Interpretation is relevant to the SFUG:

I-0244	Flexibility in packaging SFUG

The following Interpretations are relevant to the TFM:

I-0046	Detailed audit record structure
I-0069	Flexibility in packaging TFM

The following Interpretations are relevant to design documentation:

I-0192	Interface manuals as design documentation
I-0193	Standard system books as design documentation

None of the Interpretations are relevant to test documentation.

DDOC88 National Computer Security Center, *A Guide to Understanding Design Documentation in Trusted Systems*, NCSC-TG-007, Version 1, 2 October 1988.

This document provides guidance on TCSEC design documentation requirements and what documentation is expected by the evaluation team in the review process and for deliverables. By accurately describing the design of a system, the guideline states that design documentation provides assurance that there is an understanding of how and why the system

provides trust, and enables developers to determine that proposed changes to the system do not affect trustworthiness.

SFUG91 National Computer Security Center, *A Guide to Writing the Security Features User's Guide for Trusted Systems*, NCSC-TG-026, Version 1, September 1991.

This document explains the motivation and meaning of the TCSEC requirement for an SFUG. It identifies and discusses the considerations that influence the development and evaluation of an SFUG, such as its audience, content, and organization. It discusses various approaches to writing an SFUG that have been accepted by trusted product evaluators in the past.

STTD93 National Computer Security Center, *A Guide to Understanding Security Testing and Test Documentation in Trusted Systems*, NCSC-TG-023, Version 1, July 1993.

This document provides guidance on documenting test philosophy, plans, procedures and results at all TCSEC classes. It includes examples of test plans and considers covert channel testing. At C2 and B1, the documentation guidance in this guide is superseded by [VTD94].

TFM92 National Computer Security Center, *Guidelines for Writing Trusted Facility Manuals*, NCSC-TG-016, Version 1, October 1992.

This document explains the motivation and meaning of the TCSEC requirement for a TFM. It identifies and discusses the considerations that influence the development and evaluation of a TFM, such as its audience, content, and organization. It discusses various approaches to writing a TFM that have been accepted by trusted product evaluators in the past.

VDD94 National Computer Security Center, *Form and Content of Vendor Design Documentation*, Draft, May 1994.

This document specifies additional design documentation requirements for the evaluation process at C2 and B1. Three summary documents, the Architecture Summary Document (ASD), the Interface Summary Document (ISD), and anextended Philosophy of Protection (PoP) must be submitted by a vendor prior to the IPTR. The required content and recommended organization of the summary documents are stated and illustrated with examples.

VTD94 National Computer Security Center, *Form and Content of Vendor Test Documentation*, Draft, May 1994.

This document specifies additional test documentation requirements for the evaluation process at C2 and B1. A Test Matrix Document (TMD) and portions of the TCSEC test documentation must be submitted by a vendor prior to the Intensive Preliminary Technical Review (IPTR). The required

content and recommended organization of the TMD is defined and guidance is supplied concerning the documentation of test plans, procedures and results.

Supplemental Readings

Sullivan89 Sullivan, E., “What is a Trusted System Anyway?,” *Proceedings of SHARE72*, July 1989.

Documentation required and useful for a trusted system is reviewed. << Note: This paper is included as a required reading in Module 13. >>

TFM89 National Computer Security Center, *A Guide to Understanding Trusted Facility Management*, NCSC-TG-015, Version 1, 18 October 1989.

This document provides useful insights into the trusted facility management requirements of the TCSEC and hence sample topics to be addressed within the TFM.

Other Readings

None.